Computing the Matched Filter in Linear Time

To Solomon Golomb for the occasion of his 80 birthday mazel tov

Alexander Fish
Department of Mathematics
University of Wisconsin
Madison, WI 53706, USA
Email: afish@math.wisc.edu

Shamgar Gurevich
Department of Mathematics
University of Wisconsin
Madison, WI 53706, USA
Email: shamgar@math.wisc.edu

Ronny Hadani
Department of Mathematics
University of Texas
Austin, TX 78712, USA
Email: hadani@math.utexas.edu

Akbar Sayeed
Department of Electrical Engineering
University of Wisconsin
Madison, WI 53706, USA
Email: akbar@engr.wisc.edu

Oded Schwartz
Department of Computer Science
University of California
Berkeley, CA 94720, USA
Email: odedsc@eecs.berkeley.edu

***Abstract*—A fundamental problem in wireless communication is the *time-frequency shift* (TFS) problem: Find the time-frequency shift of a signal in a noisy environment. The shift is the result of time asynchronization of a sender with a receiver, and of non-zero speed of a sender with respect to a receiver. A classical solution of a discrete analog of the TFS problem is called the *matched filter* algorithm. It uses a pseudo-random waveform $S(t)$ of the length p, and its arithemtic complexity is $O(p^2 \cdot \log(p))$, using fast Fourier transform. In these notes we introduce a novel approach of designing new waveforms that allow faster matched filter algorithm. We use techniques from group representation theory to design waveforms $S(t)$, which enable us to introduce two *fast matched filter* (FMF) algorithms, called the *flag algorithm*, and the *cross algorithm*. These methods solve the TFS problem in $O(p \cdot \log(p))$ operations. We discuss applications of the algorithms to mobile communication, GPS, and radar.**

I. Introduction

Denote by $\mathcal{H} = \mathbb{C}(\mathbb{F}_p)$ the vector space of complex valued functions on the finite field $\mathbb{F}_p = \{0, 1, ..., p-1\}$, where addition and multiplication is done modulo the odd prime number p. The vector space $\mathcal{H}$ is equipped with the standard inner product $\langle f_1, f_2 \rangle = \sum_{t \in \mathbb{F}_p} f_1(t)\overline{f_2(t)}$, for $f_1, f_2 \in \mathcal{H}$, and will be referred to as the *Hilbert space of digital signals*.

Let us start with a motivational problem.

A. Mobile communication problem

We consider the following mathematical model of mobile communication [10]. There exists a collection of users $j = 1, ..., r$, each holding a bit $b_j \in \{\pm 1\}$, and a private signal $S_j \in \mathcal{H}$. User j transmits its message $b_j \cdot S_j$ to a base station (antenna), and the base station receives the superposition sum

$$R(t) = \sum_{j=1}^{r} b_j \cdot e^{\frac{2\pi i}{p}\omega_j \cdot t} \cdot S_j(t + \tau_j) \ + \mathcal{W}(t), \quad t \in \mathbb{F}_p, \quad \text{(I.1)}$$

where $\mathcal{W} \in \mathcal{H}$ denotes a random white noise of mean zero, τ_j encodes the time asynchronization of user j with the base station, ω_j encodes the radial velocity of user j with respect to the base station, and $i = \sqrt{-1}$.

The base station "knows" the signals S_j's and R. The objective is:

Problem I.1 (Mobile communication problem): Extract the bits b_j, $j = 1, ..., r$.

A resolution of Problem I.1 will be deduced (see Section I-F) from our solution to the following problem.

B. The time-frequency shift (TFS) problem

We have r signals $S_j \in \mathcal{H}$, $j = 1, ..., r$, called the *sender* waveforms. Additionally, we are given the *receiver* waveform $R \in \mathcal{H}$, which satisfies

$$R(t) = \sum_{j=1}^{r} e^{\frac{2\pi i}{p}\omega_j \cdot t} \cdot S_j(t + \tau_j) \ + \mathcal{W}(t), \quad t \in \mathbb{F}_p, \quad \text{(I.2)}$$

where $\mathcal{W} \in \mathcal{H}$ denotes a random white noise of mean zero, and $(\tau_j, \omega_j) \in \mathbb{F}_p \times \mathbb{F}_p$, $j = 1, ..., r$. We will call the pairs (τ_j, ω_j) the *time-frequency shifts*, and the vector space $V = \mathbb{F}_p \times \mathbb{F}_p$ the *time-frequency plane*.

The precise formulation of the *time-frequency shift problem* is the following:

Problem I.2 (TFS problem): Given the waveforms S_j, $j = 1, ..., r$, and R, extract the time-frequency shifts $(\tau_j, \omega_j) \in V$, $j = 1, ..., r$.

C. The matched filter (MF) algorithm

A classical solution [3], [4], [5], [7], [10], [11], [12] to Problem I.2, is the *matched filter algorithm*. For a fixed $k \in \{1, ..., r\}$, we define the following matched filter (MF) matrix of the sender S_k, and the receiver R:

$$\mathcal{M}[S_k, R](\tau, \omega) = \left\langle e^{\frac{2\pi i}{p}\omega \cdot t} \cdot S_k(t + \tau), R(t) \right\rangle, \quad (\tau, \omega) \in V. \quad \text{(I.3)}$$

A direct verification shows that for $\zeta_j = e^{\frac{2\pi i}{p}(\tau\omega_j - \omega\tau_j)}$, $j = 1, ..., r$, we have

$$\begin{aligned}\mathcal{M}[S_k, R](\tau, \omega) &= \zeta_k \cdot \mathcal{M}[S_k, S_k](\tau - \tau_k, \omega - \omega_k) \\ &+ \sum_{j \neq k} \zeta_j \cdot \mathcal{M}[S_k, S_j](\tau - \tau_j, \omega - \omega_j) \\ &+ O(\frac{NSR}{\sqrt{p}}),\end{aligned} \quad \text{(I.4)}$$

where $NSR = \frac{1}{SNR}$ is the inverse of the signal-to-noise ratio between the waveform S_k and $\mathcal{W}$. For simplicity, we assume that the NSR is not too large, and, for the rest of the paper, we will omit the last term in (I.4).

In order to extract the time-frequency shift (τ_k, ω_k), using the matched filter, it is "standard" (see [3], [4], [5], [7], [10], [11], [12]) to use almost-orthogonal pseudo-random signals $S_j \in \mathcal{H}$ of norm one. Namely, all the summands in right-hand side of (I.4) are of size $O(\frac{1}{\sqrt{p}})$, with the exception that for $(\tau, \omega) = (\tau_k, \omega_k)$ we have $\mathcal{M}[S_k, S_k](\tau - \tau_k, \omega - \omega_k) = 1$. Hence,

$$|\mathcal{M}[S_k, R](\tau, \omega)| = \begin{cases} 1 + \varepsilon_{r,p}, & \text{if } (\tau, \omega) = (\tau_k, \omega_k); \\ \varepsilon_{r,p}, & \text{if } (\tau, \omega) \neq (\tau_k, \omega_k), \end{cases} \quad \text{(I.5)}$$

where $\varepsilon_{r,p} = O(\frac{r}{\sqrt{p}})$.

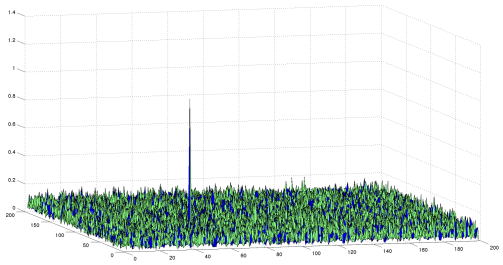

Fig. 1. $|\mathcal{M}[S_1, R]|$ *with pseudo-random* S_1, S_2, *and* $(\tau_1, \omega_1) = (50, 50)$

Identity (I.5) suggests the following "entry-by-entry" algorithmic solution to TFS problem: Compute the matrix $\mathcal{M}[S_k, R]$, and choose (τ_k, ω_k) for which $|\mathcal{M}[S_k, R](\tau_k, \omega_k)| \approx 1$. However, this solution of TFS problem is very expensive in terms of arithmetic complexity, i.e., the number of arithmetic (multiplication, and addition) is $O(r \cdot p^3)$. One can do better using a "line-by-line" computation. This is due to the next observation.

Remark I.3 (FFT): The restriction of the matrix $\mathcal{M}[S_k, R]$ to any line (not necessarily through the origin) in the time-frequency plane V, is a convolution that can be computed, using the fast Fourier transform algorithm (FFT), in $O(p \cdot \log(p))$ arithmetic operations.

As a consequence of Remark I.3, one can solve TFS problem in $O(r \cdot p^2 \cdot \log(p))$ arithmetic operations. To the best of our knowledge, the "line-by-line" computation is also the fastest method which exists in the literature [9]. Note that computing one entry in $\mathcal{M}[S_k, R]$ costs already $O(p)$ operations. This leads to the following *fast matched filter (FMF)* problem:

Problem I.4 (FMF problem): Design waveforms $S_j \in \mathcal{H}$, $j = 1, ..., r$, to solve TFS problem in almost linear time for shift.

D. *The flag method*

We introduce the *flag method* to propose a solution to FMF problem. We will show how to associate with the $p+1$ lines, through $(0, 0)$ in the time-frequency plane, L_j, $j = 1, ..., p+1$, a system of almost orthogonal waveforms $S_{L_j} \in \mathcal{H}$, that we will call *flags*. The system satisfies

$$|\mathcal{M}[S_{L_k}, R](\tau, \omega)| = \begin{cases} 2 + \varepsilon_{r,p}, & \text{if } (\tau, \omega) = (\tau_k, \omega_k); \\ 1 + \varepsilon_{r,p}, & \text{if } (\tau, \omega) \in L'_k \setminus (\tau_k, \omega_k); \\ \varepsilon_{r,p}, & \text{if } (\tau, \omega) \in V \setminus L'_k, \end{cases} \quad \text{(I.6)}$$

where $\varepsilon_{r,p} = O(\frac{r}{\sqrt{p}})$, R is the receiver waveform (I.2), defined with respect to any r flags containing S_{L_k}, and L'_k is the shifted line $L_k + (\tau_k, \omega_k)$.

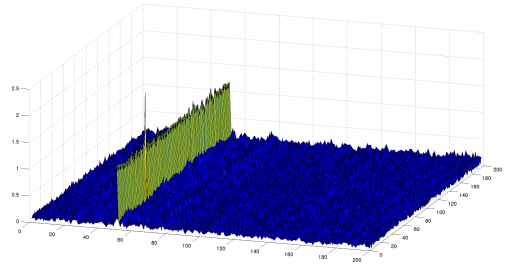

Fig. 2. $|M[S_{L_1}, R]|$ *with two flags* S_{L_1}, S_{L_2}, *and* $(\tau_1, \omega_1) = (50, 50)$

Identity (I.6) suggests the "flag" algorithmic solution to FMF problem in the case that the number of waveforms $r \ll \sqrt{p}$, and p is sufficiently large. In the following we assume that R and S_{L_k} are as in (I.6).

Algorithm I.5 (Flag algorithm):

- Choose a line $L_k^{\perp}$ different from L_k.
- Compute $\mathcal{M}[S_{L_k}, R]$ on $L_k^{\perp}$. Find (τ, ω) such that $|\mathcal{M}[S_{L_k}, R](\tau, \omega)| \approx 1$, i.e., (τ, ω) on the shifted line $L_k + (\tau_k, \omega_k)$.
- Compute $\mathcal{M}[S_{L_k}, R]$ on $L_k + (\tau_k, \omega_k)$ and find (τ, ω) such that $|\mathcal{M}[S_{L_k}, R](\tau, \omega)| \approx 2$.

The arithmetic complexity of the flag algorithm is $O(r \cdot p \log(p))$, using the FFT (Remark I.3).

E. *The cross method*

Another solution to the TFS problem, and subsequently to the mobile communication problem, is the *cross method*. The idea is similar to the flag method, i.e., first to find a line on

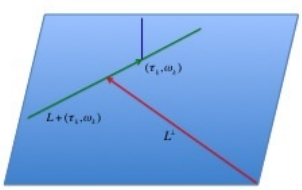

Fig. 3. Diagram of the flag algorithm

which the time-frequency shift is located, and then to search on the line to find the time-frequency shift. We will show how to associate with the $\frac{p+1}{2}$ distinct pairs of lines $L, M \subset V$ a system of almost-orthogonal waveforms $S_{L,M}$, that we will call *crosses*. The system satisfies

$$|\mathcal{M}[S_{L,M}, R]| = \begin{cases} 2+\varepsilon_{r,p}, & \text{if } (\tau,\omega)=(\tau_{L,M},\omega_{L,M}); \\ 1+\varepsilon_{r,p}, & \text{if } (\tau,\omega)\in(L'\cup M')\setminus(\tau_{L,M},\omega_{L,M}); \\ \varepsilon_{r,p}, & \text{if } (\tau,\omega)\in V\setminus(L'\cup M'), \end{cases}$$

where $\varepsilon_{r,p} = O(\frac{r}{\sqrt{p}})$, R is the receiver waveform (I.2), defined with respect to any r different crosses containing $S_{L,M}$, and $L' = L + (\tau_{L,M}, \omega_{L,M})$, $M' = M + (\tau_{L,M}, \omega_{L,M})$.

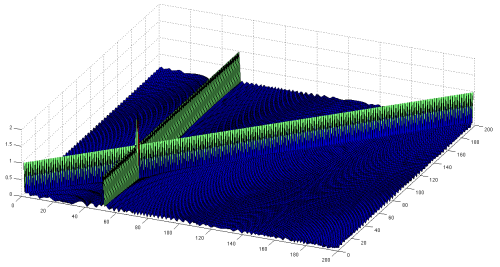

Fig. 4. $|\mathcal{M}[S_{L_1,M_1}, R]|$ with crosess S_{L_1,M_1}, S_{L_2,M_2}, and $(\tau_1, \omega_1) = (50, 50)$

The arithmetic complexity of the cross method is $O(r \cdot p\log(p))$, using the FFT (Remark I.3).

F. *Solution to the mobile communication problem*

Looking back to Problem I.1, we see that the flag and cross algorithms suggest a fast $O(r \cdot p \cdot \log(p))$ solution to extract ALL the bits b_k. Indeed, identity (I.4) implies that $b_k \approx \mathcal{M}[S_k, R](\tau_k, \omega_k)/2, \quad k = 1, ..., r$, where R is the waveform (I.1), with $S_j = S_{L_j}$, $j = 1, ..., r$, for the flag method, or $S_j = S_{L_j,M_j}$, $j = 1, ..., r$, for the cross method, and $r \ll \sqrt{p}$.

II. The Heisenberg–Weil flag system

The flag waveforms, that play the main role in the flag algorithm, are of a special form. Each of them is a sum of a pseudorandom signal and a structural signal. The first has the MF matrix which is almost delta function at the origin, and the MF matrix of the second is supported on a line. The designs of these waveforms are done using group representation theory. The pseudorandom signals are designed [4], [5], [12] using the Weil representation, and will be called Weil (peak) signals[1]. The structural signals are designeded [6], [7] using the Heisenberg representation, and will be called Heisenberg (lines) signals. We will call the collection of all flag waveforms, the Heisenberg–Weil flag system. In this section we briefly recall constructions, and properties of these waveforms. A more comprehensive treatment, including proofs, will appear in [2].

A. *The Heisenberg (lines) system*

Consider the following collection of unitary operators, called Heisenberg operators, that act on the Hilbert space of digital signals:

$$\begin{cases} \pi(\tau,\omega) : \mathcal{H} \to \mathcal{H}, \quad \tau, \omega \in \mathbb{F}_p; \\ \pi(\tau,\omega) = \mathrm{M}_\omega \circ \mathrm{L}_\tau, \end{cases} \tag{II.1}$$

where $\mathrm{L}_\tau[f](t) = f(t+\tau)$ is the time-shift operator, $\mathrm{M}_\omega[f](t) = e^{\frac{2\pi i}{p}\omega\cdot t} \cdot f(t)$ is the frequency-shift operator, for every $f \in \mathcal{H}$, $t \in \mathbb{F}_p$, and $\circ$ denotes composition of operators.

The operators (II.1) do not commute in general, but rather obey the Heisenberg commutation relations $\pi(\tau,\omega) \circ \pi(\tau',\omega') = e^{\frac{2\pi i}{p}(\tau\omega'-\omega\tau')} \cdot \pi(\tau',\omega') \circ \pi(\tau,\omega)$. The expression $\tau\omega' - \omega\tau'$ vanishes if (τ,ω), (τ',ω') belong to the same line. Hence, for a given line $L \subset V = \mathbb{F}_p \times \mathbb{F}_p$ we have a commutative collection of unitary operators

$$\pi(\ell) : \mathcal{H} \to \mathcal{H}, \ \ell \in L. \tag{II.2}$$

We use the theorem from linear algebra about simultaneous diagonalization of commuting unitary operators, and obtain [6], [7] a natural orthonormal basis $\mathcal{B}_L \subset \mathcal{H}$ consisting of common eigenfunctions for all the operators (II.2). The system of all such bases $\mathcal{B}_L$, where L runs over all lines through the origin in V, will be called the *Heisenberg (lines) system*. We will need the following result [6], [7]:

Theorem II.1: The Heisenberg system satisfies the properties

1) *Line.* For every line $L \subset V$, and every $f_L \in \mathcal{B}_L$, we have
$$|\mathcal{M}[f_L, f_L](\tau,\omega)| = \begin{cases} 1, & \text{if } (\tau,\omega) \in L; \\ 0, & \text{if } (\tau,\omega) \notin L. \end{cases}$$
2) *Almost-orthogonality.* For every two lines $L_1 \neq L_2 \subset V$, and every $f_{L_1} \in \mathcal{B}_{L_1}$, $f_{L_2} \in \mathcal{B}_{L_2}$, we have
$$|\mathcal{M}[f_{L_1}, f_{L_2}](\tau,\omega)| = \frac{1}{\sqrt{p}},$$
for every $(\tau,\omega) \in V$.

[1]For the purpose of the Flag method, other pseudorandom signals may work.

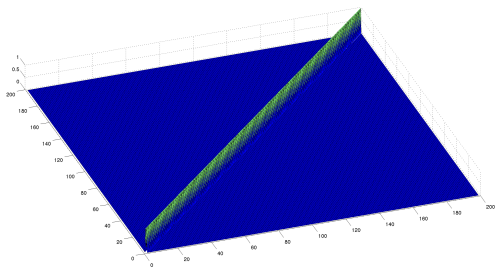

Fig. 5. $|\mathcal{M}[f_L, f_L]|$ for $L = \{(\tau, \tau);\, \tau \in \mathbb{F}_p\}$

B. *The Weil (peaks) system*

Consider the following collection of matrices

$$G = SL_2(\mathbb{F}_p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix};\ a, b, c, d \in \mathbb{F}_p,\ \text{and}\ ad - bc = 1 \right\}$$

Note that G is in a natural way a *group* [1] with respect to the operation of matrix multiplication. It is called the *special linear group* of order two over $\mathbb{F}_p$. Each element $g \in G$ acts on the time-frequency plane V via the change of coordinates $v \mapsto g \cdot v$. For every $g \in G$, let $\rho(g)$ be a linear operator on $\mathcal{H}$ which is a solution of the following system of p^2 linear equations:

$$\Sigma_g:\ \rho(g) \circ \pi(\tau, \omega) = \pi(g \cdot (\tau, \omega)) \circ \rho(g), \quad \tau, \omega \in \mathbb{F}_p, \quad \text{(II.3)}$$

where π is defined by (II.1). Denote by $\mathrm{Sol}(\Sigma_g)$ the space of all solutions to System (II.3). The following is a basic result [13]:

Theorem II.2 (Stone–von Neumann–Schur-Weil): There exist a unique collection of solutions $\{\rho(g) \in \mathrm{Sol}(\Sigma_g);\, g \in G\}$, which are unitary operators, and satisfy the homomorphism condition $\rho(g \cdot h) = \rho(g) \circ \rho(h)$.

Denote by $U(\mathcal{H})$ the collection of all unitary operators on the Hilbert space of digital signals $\mathcal{H}$. Theorem II.2 establishes the map $\rho : G \to U(\mathcal{H})$, which is called the *Weil representation* [13]. The group G is not commutative, but contains a special class of maximal commutative subgroups called tori[2] [4], [5]. Each torus $T \subset G$ acts via the Weil representation operators

$$\rho(g) : \mathcal{H} \to \mathcal{H}, \quad g \in T. \quad \text{(II.4)}$$

This is a commutative collection of diagonalizable operators, and it admits [4], [5] a natural orthonormal basis $\mathcal{B}_T$ for $\mathcal{H}$, consisting of common eigenfunctions. The system of all such bases $\mathcal{B}_T$, where T runs over all tori in G, will be called the *Weil (peaks) system*. We will need the following result [4], [5]:

Theorem II.3: The Weil system satisfies the properties

1) *Peak.* For every torus $T \subset G$, and every $\varphi_T \in \mathcal{B}_T$, we have

$$|\mathcal{M}[\varphi_T, \varphi_T](\tau, \omega)| = \begin{cases} 1, & \text{if } (\tau, \omega) = (0, 0); \\ \leq \frac{2}{\sqrt{p}}, & \text{if } (\tau, \omega) \neq (0, 0). \end{cases}$$

[2]There are order of p^2 tori in $SL_2(\mathbb{F}_p)$.

2) *Almost-orthogonality.* For every two tori $T_1,\ T_2 \subset G$, and every $\varphi_{T_1} \in \mathcal{B}_{T_1},\ \varphi_{T_2} \in \mathcal{B}_{T_2}$, with $\varphi_{T_1} \neq \varphi_{T_2}$, we have

$$\left|\mathcal{M}[\varphi_{T_1}, \varphi_{T_2}](\tau, \omega)\right| \leq \begin{cases} \frac{4}{\sqrt{p}}, & \text{if } T_1 \neq T_2; \\ \frac{2}{\sqrt{p}}, & \text{if } T_1 = T_2, \end{cases}$$

for every $(\tau, \omega) \in V$.

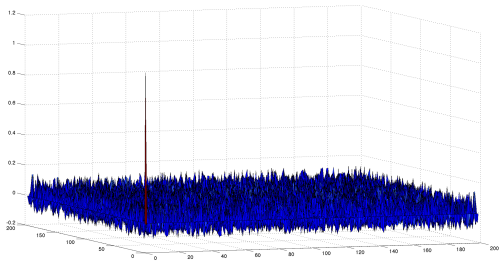

Fig. 6. $\mathcal{M}[\varphi_T, \varphi_T]$ for $T = \{\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}; 0 \neq a \in \mathbb{F}_p\}$

C. *The Heisenberg–Weil system*

We define the *Heisenberg–Weil system* of waveforms. This is the collection of signals in $\mathcal{H}$, which are of the form $S_L = f_L + \varphi_T$, where f_L and φ_T are Heisenberg and Weil waveforms, respectively. The main technical result of this paper is:

Theorem II.4: The Heisenberg–Weil system satisfies the properties

1) *Flag.* For every line $L \subset V$, torus $T \subset G$, and every flag $S_L = f_L + \varphi_T$, with $f_L \in \mathcal{B}_L,\ \varphi_T \in \mathcal{B}_T$, we have

$$|\mathcal{M}[S_L, S_L](\tau, \omega)| = \begin{cases} 2 + \epsilon_p, & \text{if } (\tau, \omega) = (0, 0); \\ 1 + \varepsilon_p, & \text{if } (\tau, \omega) \in L \setminus (0, 0); \\ \varepsilon_p, & \text{if } (\tau, \omega) \in V \setminus L, \end{cases}$$

where $|\epsilon_p| \leq \frac{4}{\sqrt{p}}$, and $|\varepsilon_p| \leq \frac{6}{\sqrt{p}}$.

2) *Almost-orthogonality.* For every two lines $L_1 \neq L_2 \subset V$, tori $T_1,\ T_2 \subset G$, and every two flags $S_{L_j} = f_{L_j} + \varphi_{T_j}$, with $f_{L_j} \in \mathcal{B}_{L_j},\ \varphi_{T_j} \in \mathcal{B}_{T_j},\ j = 1, 2,\ \varphi_{T_1} \neq \varphi_{T_2}$, we have

$$|\mathcal{M}[S_{L_1}, S_{L_2}](\tau, \omega)| \leq \begin{cases} \frac{9}{\sqrt{p}}, & \text{if } T_1 \neq T_2; \\ \frac{7}{\sqrt{p}}, & \text{if } T_1 = T_2, \end{cases}$$

for every $(\tau, \omega) \in V$.

A proof of Theorem II.4 will appear in [2].

Remark II.5: As a consequence of Theorem II.4 we obtain families of $p + 1$ almost-orthogonal flag waveforms which can be used for solving the TFS and mobile communication problems in almost linear time.

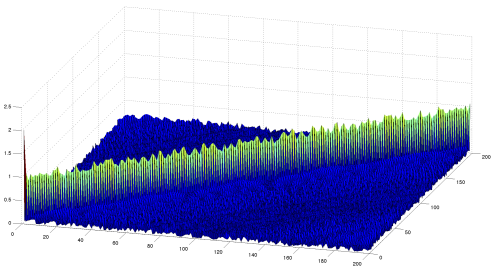

Fig. 7. $|\mathcal{M}[S_L, S_L]|$ for Heisenberg–Weil flag with $L = \{(\tau, \tau);\ \tau \in \mathbb{F}_p\}$

III. The Heisenberg cross system

We define the *Heisenberg cross system* of waveforms. This is the collection of signals in $\mathcal{H}$, which are of the form $S_{L,M} = f_L + f_M$, where f_L, f_M, $L \neq M$, are Heisenberg waveforms defined in Section II-A. The following follows immediately from Theorem II.1:

Theorem III.1: The Heisenberg cross system satisfies the properties

1) *Cross.* For every pair of distinct lines $L, M \subset V$, and every cross $S_{L,M} = f_L + f_M$, with $f_L \in \mathcal{B}_L$, $f_M \in \mathcal{B}_M$, we have

$$|\mathcal{M}[S_{L,M}, S_{L,M}](\tau,\omega)| = \begin{cases} 2+\varepsilon_p, & \text{if } (\tau,\omega)=(0,0); \\ 1+\varepsilon_p, & \text{if } (\tau,\omega)\in(L\cup M)\setminus(0,0); \\ \varepsilon_p, & \text{if } (\tau,\omega)\in V\setminus(L\cup M), \end{cases}$$

where $|\varepsilon_p| \leq \frac{2}{\sqrt{p}}$.

2) *Almost-orthogonality.* For every four distinct lines $L_1, M_1, L_2, M_2 \subset V$, and every two crosses $S_{L_j,M_j} = f_{L_j} + f_{M_j}$, $j = 1, 2$, we have

$$\left|\mathcal{M}[S_{L_1,M_1}, S_{L_2,M_2}](\tau,\omega)\right| \leq \frac{4}{\sqrt{p}}.$$

for every $(\tau, \omega) \in V$.

Remark III.2: As a consequence of Theorem III.1 we obtain families of $\frac{p+1}{2}$ almost-orthogonal cross waveforms which can be used for solving the TFS and mobile communication problems in almost linear time.

IV. Applications to GPS and radar

In the introduction we described application of flag and cross methods to mobile communication. In this section we demonstrate applications to global positioning system (GPS), and discrete radar.

A. Application to global positioning system (GPS)

The model of GPS works as follows [8]. A client on the earth surface wants to know his geographical location. Satellites $j = 1, ..., r$ send to earth their location. For simplicity, the location of satellite j is a bit $b_j \in \{\pm 1\}$. Satellite j transmits to the earth its signal $S_j \in \mathcal{H}$ multiplied by its location b_j. The client receives the signal

$$R(t) = \sum_{j=1}^{r} b_j \cdot e^{\frac{2\pi i}{p}\omega_j \cdot t} \cdot S_j(t + \tau_j) \ + \mathcal{W}(t),$$

where ω_j encodes the radial velocity of satellite j with respect to the client, τ_j encodes the distance between satellite j and the client[3], and $\mathcal{W}$ is a random white noise of mean zero.

Problem IV.1 (GPS problem): Find (b_j, τ_j), $j = 1, ..., r$.

By using Heisenberg–Weil or Heisenberg cross waveforms we find the pairs (b_j, τ_j) in $O(r \cdot p\log(p))$ arithmetical operations.

B. Application to discrete radar

The model of discrete radar works as follows [7]. A radar sends a waveform $S \in \mathcal{H}$ which bounds back by r targets. The signal $R \in \mathcal{H}$ which is received as an echo has the form[4]

$$R(t) = \sum_{j=1}^{r} e^{\frac{2\pi i}{p}\omega_j \cdot t} \cdot S(t + \tau_j) \ + \mathcal{W}(t),$$

where ω_j encodes the radial velocity of target j with respect to the radar, τ_j encodes the distance between target j and the radar, and $\mathcal{W}$ is a random white noise of mean zero.

Problem IV.2 (Discrete radar problem): Find (τ_j, ω_j), $j = 1, ..., r$.

By sending Heisenberg–Weil waveform $S_L = f_L + \varphi_T$ we get[5]

$$|\mathcal{M}[S_L, R](\tau,\omega)| = \begin{cases} 2 + \varepsilon_{r,p}, \text{ if } (\tau,\omega) \in \{(\tau_j,\omega_j)\}; \\ 1 + \varepsilon_{r,p}, \text{ if } (\tau,\omega) \in L + (\tau_j,\omega_j) \setminus (\tau_j,\omega_j); \\ \varepsilon_{r,p}, \text{ otherwise,} \end{cases}$$

where $\varepsilon_{r,p} = O(\frac{r}{\sqrt{p}})$.

This means that by using the flag algorithm we solve the radar problem in $O(r \cdot p\log(p))$ arithmetical operations.

Remark IV.3 (Important): Note that the cross method is not applicable for the discrete radar problem if the number of targets $r > 1$.

Acknowledgement. Warm thanks to Joseph Bernstein for his support and encouragement in interdisciplinary research. We are grateful to Anant Sahai, for sharing with us his thoughts, and ideas on many aspects of signal processing and wireless communication. The project described in this paper was initiated by a question of Mark Goresky and Andy Klapper during the conference SETA2008, we thank them very much. We appreciate the support and encouragement of Nigel Boston, Robert Calderbank, Solomon Golomb, Guang Gong, Olga Holtz, Roger Howe, Peter Sarnak, Nir Sochen, and Alan Weinstein.

[3] From the τ_j we can find [8] the distance between satellite j and the client, given that $r \geq 4$ and the clocks of all satellites are synchronized.

[4] In practice there are intensity coefficients $0 \leq \alpha_j \leq 1$ such that $R(t) = \sum_{j=1}^{r} \alpha_j \cdot e^{\frac{2\pi i}{p}\omega_j \cdot t} \cdot S(t+\tau_j) + \mathcal{W}(t)$. Assuming that α_j's are sufficiently large our methods are applicable verbatim.

[5] For simplicity we assume that all the shifted lines $L + (\tau_j, \omega_j)$'s are distinct. The general case is treated similarly.

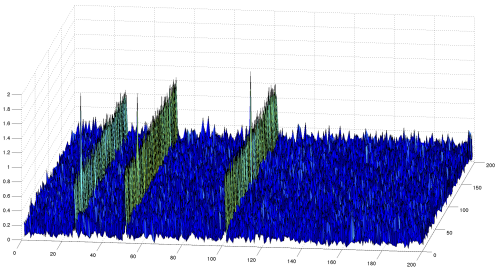

Fig. 8. $|\mathcal{M}[S_L, R]|$ with $L = \{(\tau, 0);\ \tau \in \mathbb{F}_p\}$, and shifts $(50, 50)$, $(100, 100)$, $(150, 150)$

REFERENCES

[1] Artin M., Algebra. *Prentice Hall, Inc., Englewood Cliffs, NJ* (1991).

[2] Fish A., Gurevich S., Hadani R., Sayeed A., Schwartz O., Fast matched filter and group representation theory. *In preparation (2011).*

[3] Golomb, S.W. and Gong G., Signal design for good correlation. For wireless communication, cryptography, and radar. *Cambridge University Press, Cambridge (2005).*

[4] Gurevich S., Hadani R., Sochen N., The finite harmonic oscillator and its associated sequences. *PNAS, July 22, 2008 vol. 105 no. 29 9869–9873.*

[5] Gurevich S., Hadani R., Sochen N., The finite harmonic oscillator and its applications to sequences, communication and radar . *IEEE Transactions on Information Theory, vol. 54, no. 9, September 2008.*

[6] Howe R., Nice error bases, mutually unbiased bases, induced representations, the Heisenberg group and finite geometries. *Indag. Math. (N.S.) 16 (2005), no. 3–4, 553–583.*

[7] Howard, S. D., Calderbank, R., and Moran W., The finite Heisenberg–Weyl groups in radar and communications. *EURASIP J. Appl. Signal Process (2006).*

[8] Kaplan E., Understanding GPS Principles and Applications. *Artech house, INC (1996).*

[9] O'Toole J.M., Mesbah M., and Boashash B., Accurate and efficient implementation of the time–frequency matched filter. *IET Signal Process., 2010, Vol. 4, Iss. 4, pp. 428–437.*

[10] Tse D., and Viswanath P., Fundamentals of Wireless Communication. *Cambridge University Press (2005).*

[11] Verdu S., Multiuser Detection, *Cambridge University Press (1998).*

[12] Wang Z., and Gong G., New Sequences Design From Weil Representation With Low Two-Dimensional Correlation in Both Time and Phase Shifts. *IEEE Transactions on Information Theory, vol. 57, no. 7, July 2011.*

[13] Weil A., Sur certains groupes d'operateurs unitaires. *Acta Math. 111, 143-211 (1964).*